



Official Contractor Certification and Confidential Agreement Office of Technology Services  
(OTS)

Division of Administration  
**Office of Technology Services**  
Information Security and Compliance

**TO:** Office of Technology Services (OTS) contractors, vendors, and employees who do not have access to Louisiana Employees Online (LEO), but provide technical support services to the states information systems or data stored within them.

**FROM:** Information Security and Compliance, Division of Administration Training Coordinator.

**SUBJECT:** Required training courses for individuals who need to obtain access or recertify to maintain access to the Office of Technology Services Information Systems.

**TRAINING:** Contractors, employees, and vendors, requesting access to the State of Louisiana's Information Systems must complete Internal Revenue Service (IRS) and Cyber Security Training before access is granted. They must complete security awareness, role-based security IT training, and Cyber Security Training before beginning work and each year after completing the training for recertification. Engaging in criminal activities such as sanctions one could face if divulging in criminal activities.

The Cyber Security class reminds the contractor, employee, or vendor their role in preparing and staying current and up-to-date with evolving threats within Cyber Security. This class is a baseline understanding of common cyber security threats, vulnerabilities, and risks which provides an overview of how basic cyber-attacks are constructed and applied to real life security threats and what to do when they occur.

All employees and contractors are responsible for protecting the state's information entrusted to them. As an employee for \_\_\_\_\_ **(Print Company or Contractor Name)**, I have reviewed the OTS Information Security Policy and Procedures and received safeguard training for protecting Restricted Information **and** understand the responsibility to report improper inspection or disclosure of FTI, including breaches and security incidents to the Office of Technology Services Information Security Team. If FTI is involved, they will follow through with their procedures to notify TIGTA and Office of Safeguards.

All handling of any returns of taxpayers, other records, files of the state's data, or information derived there from within, the contractor shall recognize and acknowledge the nature of said information, and shall comply with all the confidentiality restrictions embodied in La. R.S. 47:1508. Furthermore, the Contractor should recognize that La. R.S. 47:1508.1 imposes fines and/or imprisonment upon conviction for the disclosure of information in violation of La. R.S. 47:1508.

## **CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES**

### **I. PERFORMANCE**

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

- (7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- (8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (11.) [OTS Information Security Team](#) shall be notified as soon as a security event is discovered such as vulnerabilities, Unauthorized Access, Information Spillage, or any other events that are discovered.

## **II. CRIMINAL/CIVIL SANCTIONS**

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure.

These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR301.6103(n)-1.

- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any

manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

- (3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see [Exhibit 4 Sanctions for Unauthorized Disclosure](#), and [Exhibit 5, Civil Damages for Un-Authorized Disclosure](#)). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See [Section 10](#)) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

### III. INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and

operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Contractors, employees, and vendors are required to notify the [OTS Information Security Team](#) for all security incidents, breaches, or notifications that may need further investigation or notification to Treasury Inspector General for Tax Administration (TIGTA) or Office of Safeguards to meet the required 24 hours incident response requirement.

All contractors who perform work for the State of Louisiana, State Agency, or Subcontracted are notified that violation of the above Federal and/or State Laws or failure to report a security incident potentially involving state data may subject them to immediate termination of contract, or employment. In addition to termination, violation of any of these laws may subject the contractor, employee, or vendor to Federal and/or State criminal charges brought against them.

I \_\_\_\_\_ (Print Name) fully understand and have been notified of IRC laws along with the related sanctions associated with the IRC Codes listed above. I have completed training and have learned to protect restricted data from Unauthorized Disclosure and/or Inspection. I also understand it is my responsibility to report any security incidents to the Information Security Team throughout my contract with the state of Louisiana.

Any questions or concerns regarding the information listed above shall only be discussed with my direct management staff, Information Security Team, or Information Compliance Team.

Signature \_\_\_\_\_

Company Name \_\_\_\_\_

Start Date \_\_\_\_\_

Trained Date \_\_\_\_\_

### **Cyber Security Training ACT No. 155**

R.S. 42:1267, relative to cybersecurity training; to provide for the development of the training; to require all public servants to receive training; to require certain contractors to receive training; and to provide for related matters. Be it enacted by the Legislature of Louisiana: Section 1. R.S. 42:1267 is hereby enacted to read as follows:

### **Cybersecurity A.**

(1) The Department of State Civil Service shall institute, develop, conduct, and otherwise provide for training programs designed to keep state agencies safe from cyberattack. The programs shall be designed to focus on forming information; security habits and procedures that protect information resources and teach best practices for detecting, assessing, reporting, and addressing information security threats. The department may make the training available as an online course.

The office of technology services shall provide assistance to the Department of State Civil Service in the development of the training program. The cost of instituting, developing, conducting, and otherwise providing cybersecurity awareness training shall be paid in the manner established by R.S. 42:1262.

(2) The Department of State Civil Service shall make the education and training on cybersecurity developed pursuant to Paragraph (1) of this Subsection available to agencies within political subdivisions of the state at as minimal cost as possible to assist those agencies in compliance with the provisions of this Section.

### **Cybersecurity B**

(1) Each state and local agency shall identify employees or elected officials who have access to the agency's information technology assets and require those employees and elected officials to complete cybersecurity training. Each new state and local agency official or employee with access to the agency's information technology assets shall complete this training within the first thirty days of initial service or employment with the agency.

(2) The agency head shall verify and report to the Department of State Civil Service on the completion of cybersecurity training by agency employees. The agency head shall periodically require an internal review to ensure compliance.

(3)(a) An agency shall require any contractor who has access to state or local government information technology assets to complete cybersecurity training during the term of the contract and during any renewal period.

(b) Completion of cybersecurity shall be included in the terms of a contract awarded by a state or local government agency to a contractor who has access to its information technology assets.

(c) The person who oversees contract management for the agency shall report each such contractor's completion to the agency head and periodically review agency contracts to ensure compliance.

(d) The agency head shall verify and report to the Department of State Civil Service on the completion of cybersecurity training by each such contractor.

Section 2. This Act shall become effective upon signature by the governor or, if not

signed by the governor, upon expiration of the time for bills to become law without signature by the governor, as provided by Article III, Section 18 of the Constitution of Louisiana. If vetoed by the governor and subsequently approved by the legislature, this Act shall become effective on the day following such approval.

### **Required Training**

Complete the required training classes outlined below then sign, date, and send back to [Information Security and Compliance](#), to keep on file for required retention period.

**Note:** Cyber Security Training the Survey Must Be Completed to receive Credits for the training Class.

### **Safeguarding IRS Confidential Information – A Guide for Contractors**

### **Protecting Federal Tax Information: A Message from the IRS**

### **Protecting Federal Tax Information for Contractors (Pub. 4465-A) (Print and Keep)**

### **Cyber Security Training**

By signing this agreement, I understand upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving FTI. I watched Cyber Security Training and completed the survey at the end of the class. I also understand the penalty provisions of IRC 7431, 7213 and 7213A

Signature \_\_\_\_\_

Company Name \_\_\_\_\_

Start Date \_\_\_\_\_

Trained Date \_\_\_\_\_